

JP-A-H7-182112 discloses:

Purpose: To provide a data processor which contains a secret protecting function of writing data to a replaceable storage medium to enable even another processor to read the file data out of the storage medium.

Constitution: A data processor is provided with a coding means which codes the file management data recorded on a replaceable storage medium, and a decoding means which decodes the coded data. Then a reading/writing means is added to write or read the uncoded data into or out of the medium. Thus the data decoded by the means are recorded on the medium by the means. When a user approves to read the file data by another data processor, the data coded in the medium are decoded. Then the coded data that can be read by another data processor are recorded on the medium by the means.

The data are encoded using a value randomly written, with respect to a byte, based on a encoding table.

(19) 日本國特許庁 (JP) (22) 公開特許公報 (A) (11) 特許出願公開番号 特開平7-182112

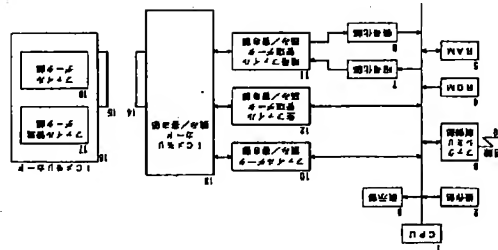
(51) Int.Cl. <sup>8</sup> G 06 F 3/06 G 11 B 20/10 20/12	識別記号 304 H H 7738-5D 9285-5D	片内整理番号 - F I	審査請求 未請求 請求項の数 6 F D (全 8 項)	技術表示箇所
(21) 出願番号 昭平5-348049 平成5年(1993)12月24日	(71) 出願人 000005321 松下電器産業株式会社 大阪府門真市大字門真1006番地 豊田 清 大阪府門真市大字門真1006番地 松下電器 産業株式会社内 (72) 発明者 (74) 代理人 井理士 役 昌明 (外1名)			
(22) 出願日				

## (54) 【発明の名称】 機密保護機能を持つデータ処理装置

【哮喘】(25)

【目的】他の装置でも可換記憶媒体のフアイルデータ交換機構を備えたデータ処理装置を提供する。

【構成】 可換記憶媒体16に記録されるファイル管理データ17の暗号化手段7と、暗号化されたファイル管理データ17の復号化手段8とを備えるデータ処理装置において、暗号化されたファイル管理データを可換記憶媒体16に書き込まない又は読出し読み手手段12を設け、復号化手段8で復号化したファイル管理データを読み手手段10で読出し、復号化手段12で可換記憶媒体16に記録する。ユーザが、他のデータ処理装置でファイルデータを読むことを認める場合は、可換記憶媒体16の暗号化されたファイル管理データが復号された後、読み手手段12を通じて、この復号された他の装置でも読める状態のファイル管理データが可換記憶媒体16に記録される。



## 【特許請求の範囲】

【請求項1】 可換記憶媒体に記録するファイル管理データを含むデータを暗号化する暗号化手段と、暗号化された前記ファイルを復号化する復号化手段とを備える、換

標準化されていない前記ファイル管理データは前記可換記憶媒体に書き込まれた読出し読み／書き手段を設け、前記復号化手段によって復号化された前記ファイル管理データを前記読出し／書き手段により前記可換記憶媒体に記録できるように構成したことを特徴とするデータ処理装置。

【請求項2】 パスワードを入力する入力手段を設け、前記パスワードが入力されたときに、前記読み/書き手段が読み取られた前記ファイル管理データを前記可換記憶媒体に記録するように構成したことを特徴とする請求項1に記載のデータ処理装置。

【請求項3】 前記可換記憶媒体が装着されたことを検知する検知手段を設け、前記検知手段の検知に応じて、前記前記暗号化手段を起動し、暗号化された前記ファイル管理データを前記可換記憶媒体に記憶させることを特徴とする請求項1または2に記載のデータ処理装置。

【請求項4】 前記暗号化手段が、暗号化データーと、前記暗号化データーに書込まれた値と前記ファイル管理データーの値とを演算して暗号化されたファイル管理データーの値を生成する演算手段とを備えることを特徴とする請求項1乃至3に記載のデータ処理装置。

【請求項5】 前記暗号化データが、各バイト毎に改入されたランダムな値を有し、前記計算手段が、前記ファイル管理データの各バイト毎の値の大きさに応じて、該ファイル管理データの値と前記暗号化データの値とを加算または減算し、前記加算または減算の別を前記暗号化データに残すことを特徴とする請求項4に記載のデータ処理装置。

【請求項6】 前記暗号化手段が、前記可換記述媒体へのファイル管理データの書き込み位置をずらす手段によって構成されることを特徴とする請求項1に記載のデータ処理装置。

## 【発明の詳細な説明】

【0001】  
【産業上の利用分野】本発明は、作成されたファイナルデータ40

[0002]

【従来の技術】情報化時代の昨今では、パーソナルコンピュータ等のデータ処理装置を用いて個人用のファイルを作成し、管理することが広く行なわれている。これら

にフロッピーディスクやICメモリーカード等の可換記憶媒体が使用される。可換記憶媒体は、誰でも簡単に装置から取り出すことができ、データ交換が非常に便利である。しかし、これは、逆に言えば、知られにくいデータが他人に簡単に漏れてしまう可能性も高く、そのため、可換記憶媒体に記録された個人々のデータの機密保護を如何に行なうかということが重要な問題になっている。

【0003】従来、可換記憶媒体に記憶されたファイルデータの機密を守るために、可換記憶媒体にファイルデータとは別のパスワードファイルを付加し、ユーザが入力したパスワードを照合して、一致したときのみファイルデータの抽出を許可し、パスワードが一致しなければファイルデータを抽出することができないように構成していた。しかし、この方法では、データ交換先のデータ処理装置がパスワードとの照合機能を持たない構造の場合には、可換記憶媒体のファイルデータが露出されてしま

【0004】こうした点を改善するため、特開平4-1-63768号公報には、可燃気媒体に記憶されるフアイル管理データを暗号化することによって、機密保護を図ることが提案されている。

【0005】この可換記憶媒体を扱うデータ処理装置は、図9に示すように、ディスクカートリッジ43（可換記憶媒体）のファイル管理データ44およびファイルデータ45の読出しまたは書き込みを行なうディスク読み／書き部42と、ファイルデータの読出しまたは書き込みを行なう部40と、

ファイルデータ読み、書き部40と、暗号化されたファイル管理データ41の読み出しまたは書き込みを行なう暗号ファイル管理データ読み、書き部41と、ファイル管理データの暗号化に使用される暗号化キーを記憶する暗号化キーレジスタ36と、この暗号化キーを用いてディस्क43に書き込むファイル管理データを暗号化する暗号化部37と、暗号化されたファイル管理データを解読するための復号化キーを記憶する復号化キーレジスタ39と、この復号化キーを用いてファイル管理データを解読し平文に変換する復号化部38と、操作部が暗号化キーおよび復号化キーを入力する操作部32と、この装置の動作を総合的に制御するCPU31、CPU31の実行する制御プログラムが格納されたROM34、CPU31のワーク領域として機能するRAM35と、所要の表示を行なう表示部33とを備えている。

【0006】ファイル管理データには、ファイル名、ファイルのサイズ、ロケーション（記憶場所）等が含まれる。機密保護とともに確保するために、ファイル名、また、機密保護とともに記録される場合には、その変換データを変換データとして含まれる。こうしたファイル管理データの内に含まれる、可換記憶媒体に正しくアクセスすることができなければ、可換記憶媒体に記憶されたデータがデータとして出力され、不可能になる。

【0007】この装置を使って、装着したディスプレイカー-



7

連の手順を図3のフローチャートに基づいて説明する。  
【0035】ステップ1：操作者は、データ処理装置に I Cメモリカード16を装着し、

ステップ2：操作者は、暗号化の指示を入力する。  
【0036】ステップ3：CPU1は、この指示を受け、I Cメモリカード16のファイル管理データの読み込みを指令し、生ファイル管理データ読み込み部12は、I Cメモリカード読み込み部13を介して、I Cメモリカード16のファイル管理データを読み込み、RAM5に書き込む。

【0037】ステップ4：暗号化部7は、CPU1の指令を受けて、RAM5に書き込まれた生ファイル管理データの少なくともファイル名および記憶位置のデータを暗号化する。この暗号化されたファイル管理データは、暗号ファイル管理データ読み込み部13およびI Cメモリカード読み込み部13を介して、I Cメモリカード16のファイル管理データ部17に書き込まれる。こうしてI Cメモリカード16の生ファイル管理データの暗号化が終了する。

【0038】ステップ5：ファイルデータの書き込みは、CPU1の指令に従ってファイル管理データ読み込み部10が実行し、フロッピディスク6を通じて受信した回線9からのデータを、I Cメモリカード読み込み部13を介して、I Cメモリカード16のファイル管理データ部18に記録する。このファイルデータの書き込みに伴って、RAM5に記憶されたファイル管理データの内容が変更され、変更後のファイル管理データは、暗号化部7で暗号化された後、暗号ファイル管理データ読み込み部13からI Cメモリカード読み込み部13を介して、I Cメモリカード16のファイル管理データ部17に送られ、ファイル管理データを更新する。こうしてI Cメモリカードへのファイルデータの書き込みが終了する。

【0039】ステップ6：操作者は、I Cメモリカード16に記録されたファイルデータを、機密保護機能を持たない他の装置でも読み出すようにしたいときは、操作部2からパスワードを入力する。

【0040】ステップ7：パスワードが入力されると、I Cメモリカード16の暗号化されたファイル管理データは、暗号ファイル管理データ読み込み部13に読み出され、復号化部8で生ファイル管理データに変換された後、RAM5に格納される。次いでこのファイル管理データは、生ファイル管理データ読み込み部12に読み出され、I Cメモリカード16のファイル管理データ部17に格納される。

【0041】ステップ8：この格納が終了すると、表示部3は、I Cカードを装置から抜いても良い状態にあることをユーザに表示し、ユーザはこれを確認してI Cメモリカードを抜く。

【0042】このようにI Cメモリカード16の機密化の解除は、操作者がパスワードを入力すると、装置が自動

8

的に実行する。  
【0043】（第2実施例）第2実施例のデータ処理装置では、I Cメモリカードを挿入すると、操作者が暗号化の指令を入力しなくても、自動的にI Cメモリカードのファイル管理データが暗号化される。この装置は、図4に示すように、I Cメモリカード読み込み部13にI Cメモリカードの装置を検出するカード挿入検知部19を備えている。その他の構成は、第1実施例の装置（図1）と変わらない。

【0044】この装置では、操作者がI Cメモリカード16を挿入すると、カード挿入検知部19を通じてそれを検知したCPU1が、I Cメモリカード16のファイル管理データの暗号化を指令し、図3におけるステップ3以降の動作が実行される。

【0045】なお、I Cメモリカードが挿入された後、初めてファイルアクセスが行なわれた時期を自動検知するように構成し、この自動検知の時期に合わせて暗号化を実施することも可能である。  
【0046】（第3実施例）第3実施例のデータ処理装置は、ファイル管理データの暗号化を、暗号化回路を用いず、簡単な方式によって実施している。この装置は、図5に示すように、ファイル管理データ部22は、使用する暗号化テーブル21と、暗号化の演算を実行する演算処理部20とを備えている。その他の構成は第1実施例の装置（図1）と変わらない。

【0047】暗号化テーブル21は、1バイト毎に1～127のランダムな値が収められており、演算処理部20は、この暗号化テーブル21を使って、図6に示す手順でファイル管理データを暗号化する。  
【0048】ステップ31：暗号化テーブル21の1バイト毎の値と、ファイル管理データの1バイト毎の値とを比較する。

【0049】ステップ32：ファイル管理データの値が0～127の範囲にあるかどうかを見て、ステップ33：ファイル管理データの値が0～127のときは、このデータの値から暗号化テーブルの値を減算し、その結果、得られた値をファイル管理データの値とする。

【0050】ステップ34：また、ファイル管理データの値が1～127のときは、このデータの値と暗号化テーブルの値とを加算し、その結果、得られた値をファイル管理データの値とする。

【0051】ステップ35：加算したときは暗号化テーブル21の該当する数値にマイナス符号をつけて暗号化テーブル21を更新する。

【0052】ステップ36：こうした処理をファイル管理データの暗号化すべき項目について繰り返し実施する。

9

する。こうすることにより基のファイル管理データの値が求められる。復号化の演算後は、暗号化テーブルの数値に付けたマイナス符号を取り除く。

【0053】（第4実施例）第4実施例のデータ処理装置は、ファイル管理データをI Cメモリカードのファイル管理データ部17に位置をずらして書き込むことにより、暗号化と同じ効果を上げていく。この装置は、図7に示すように、ファイル管理データ部17にファイル管理データを位置をずらして書き込みは既述している。その他のファイル管理データ位置制御部22を備えている。その他の構成は第1実施例の装置（図1）と変わらない。

【0054】この装置では、図3のステップ4における暗号化に際して、図8（a）に示すように、ファイル管理データをI Cメモリカード16のファイル管理データ部17に、位置をずらして書き込む。こうすることによりI Cメモリカード16は、本装置以外で読めなくなる。

【0055】また、このI Cメモリカード16を他の装置でも読出せるように、操作者が操作部2からパスワード20を入力した場合には、図8（b）に示すように、ステップ42：ファイル管理データ位置制御部22は、ファイル管理データ部17のずれた位置（書き込み時にずらした位置）からファイル管理データを読み込んでRAM5に書き込み。

【0056】このように、第4実施例の装置では、暗号化回路を使わずに、簡単な構成でI Cメモリカードの機密保護を実現している。  
【0057】なお、各実施例では、可換記憶媒体としてI Cメモリカードを用いているが、フロッピディスク等、他の装置・着脱可能な記憶媒体を用いることも勿論可能である。

【0058】また、先に示した従来のデータ処理装置と同じように、ファイルデータを変換キーによって変換して可換記憶媒体に書き込むと共に、この変換キーをファイル管理データの中に含めて暗号化することも可能である。  
【0059】（第5実施例）以上の実施例の説明から明らかなように、本発明のデータ処理装置は、可換記憶媒体に記憶されたファイルデータの機密を厚く保護することができ、また、ユーザが許す場合には、可換記憶媒体に記憶されたファイルデータを機密保護機能を持たないデータ処理装置で読出せるように変換することができ、この変換は、ユーザがこの装置にパスワードを入力することにより自動的に実行される。従って、ユーザ自身は、変

10

換のためのロードを特に必要としない。一方、パスワードを知らない第三者は、この変換を行なうことができず、データの機密は保護される。

【0060】また、暗号化テーブルと演算処理部を用いることにより、特別な暗号化回路を使わずに、可換記憶媒体のファイルデータの機密を保護することができ

る。  
【0061】さらに、ファイル管理データをずらして書き込むという簡便な手段によって、暗号化に相当する効果を得ることができる。

【図面の簡単な説明】  
【図1】本発明の第1実施例におけるデータ処理装置の構成を示すブロック図、

【図2】前記データ処理装置で処理されるファイル管理データの構成を示す図、

【図3】第1実施例のデータ処理装置における動作手順を示すフローチャート、

【図4】本発明の第2実施例におけるデータ処理装置の構成を示すブロック図、

【図5】本発明の第3実施例におけるデータ処理装置の構成を示すブロック図、

【図6】第3実施例のデータ処理装置における動作手順を示すフローチャート、

【図7】本発明の第4実施例におけるデータ処理装置の構成を示すブロック図、

【図8】第4実施例のデータ処理装置における暗号化（a）および復号化（b）の動作手順を示すフローチャート、

【図9】従来のデータ処理装置の構成を示すブロック図である。

【符号の説明】

1、31 CPU

2、32 操作部

3、33 表示部

4、34 ROM

5、35 RAM

6 フロッピディスク

7、37 暗号化部

8、38 復号化部

9 回線

10 ファイル管理データ読み込み部

11 暗号ファイル管理データ読み込み部

12 生ファイル管理データ読み込み部

13 I Cメモリカード読み込み部

14 データ処理装置のインターフェイス部

15 I Cカードのインポートウェア部

16 I Cメモリカード

17 ファイル管理データ部

18 ファイルデータ部

19 カード挿入検知部

